Covert Human Intelligence Sources

Draft Revised Code of Practice

Covert Human Intelligence Sources

Draft Revised Code of Practice

Presented to Parliament pursuant to section 71(9) of the Regulation of Investigatory Powers Act 2000

Covert Human Intelligence Sources
Code of Practice

Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000

Contents

1. Introduction

Definitions

1.1. In this code the:

- "1989 Act" means the Security Service Act 1989;
- "1994 Act" means the Intelligence Services Act 1994;
- "1997 Act" means the Police Act 1997;
- "2000 Act" means the Regulation of Investigatory Powers Act 2000;
- "RIP(S)A" means the Regulation of Investigatory Powers (Scotland) Act 2000;
- "2009 Order" means the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2009.

Background

1.2. This code of practice provides guidance on the authorisation of the use or conduct of covert human intelligence sources ("CHIS") by public authorities under Part II of the 2000 Act.

1.3. This code is issued pursuant to Section 71 of the 2000 Act, which stipulates that the Secretary of State shall issue one or more codes of practice in relation to the powers and duties in Parts I to III of the 2000 Act, section 5 of the 1994 Act and Part III of the 1997 Act. This code replaces the previous code of practice issued in 2002.

1.4. This code is publicly available and should be readily accessible by members of any relevant public authority seeking to use the 2000 Act to authorise the use or conduct of CHIS[1].

Effect of code

1.5. The 2000 Act provides that all codes of practice relating to the 2000 Act are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant to any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal established under the 2000 Act, or to one of the Commissioners responsible for overseeing the powers conferred by the 2000 Act, it must be taken into account. Public authorities may also be required to justify, with regard to this code, the use or granting of authorisations in general or the failure to use or grant authorisations where appropriate.

1.6. Examples are included in this code to assist with the illustration and interpretation of certain provisions. Examples are not provisions of the code, but are included for guidance only. It is not possible for theoretical examples to replicate the level of detail to be found in real cases. Consequently, authorising officers should avoid allowing superficial similarities with the examples to determine their decisions and should not seek to justify their decisions solely by reference to the examples rather than to the law, including the provisions of this code.

Scope of covert human intelligence source activity to which this code applies

1.7. Part II of the 2000 Act provides for the authorisation of the use or conduct of CHIS. The definitions of these terms are laid out in section 26 of the 2000 Act and Chapter 2 of this code.

[1] Being those listed in or added to Part I of schedule 1 of the 2000 Act.

1.8. Not all human sources of information will fall within these definitions and an authorisation under the 2000 Act will therefore not always be appropriate.

1.9. Neither Part II of the 2000 Act nor this code of practice is intended to affect the existing practices and procedures surrounding criminal participation of CHIS.

2. Covert human intelligence sources: definitions and examples

Definition of a covert human intelligence source (CHIS)

2.1. Under the 2000 Act, a person is a CHIS if:

a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c);

b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.[2]

2.2. A relationship is established or maintained for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.[3]

2.3. A relationship is used covertly, and information obtained is disclosed covertly, if and only if the relationship is used or the information is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.[4]

Scope of 'use' or 'conduct' authorisations

2.4. Subject to the procedures outlined in Chapter 3 of this Code, an authorisation may be obtained under Part II of the 2000 Act for the use or conduct of CHIS.

2.5. The use of a CHIS involves any action on behalf of a public authority to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS.[5] In general, therefore, an authorisation for use of a CHIS will be necessary to authorise steps taken by a public authority in relation to a CHIS.

2.6. The conduct of a CHIS is any conduct of a CHIS which falls within paragraph 2.1 above or is incidental to anything falling within that paragraph. In other words, an authorisation for conduct will authorise steps taken by the CHIS on behalf, or at the request, of a public authority.[6]

2.7. Most CHIS authorisations will be for both use and conduct. This is because public authorities usually take action in connection with the CHIS, such as tasking the CHIS to undertake covert action, and because the CHIS will be expected to take action in relation to the public authority, such as responding to particular tasking.

2.8. Care should be taken to ensure that the CHIS is clear on what is/is not authorised at any given time and that all the CHIS's activities are properly risk assessed. Care should also be taken to

[2] See section 26(8) of the 2000 Act
[3] See section 26(9)(b) of the 2000 Act for full definition
[4] See section 26(9)(c) of the 2000 Act for full definition
[5] See section 26(7)(b) of the 2000 Act
[6] See section 26(7)(a) of the 2000 Act

ensure that relevant applications, reviews, renewals and cancellations are correctly performed. A CHIS may in certain circumstances be the subject of different use or conduct authorisations obtained by one or more public authorities. Such authorisations should not conflict.

Circumstances in which it would be appropriate to authorise the use or conduct of a CHIS

2.9. Public authorities are not required by the 2000 Act to seek or obtain an authorisation just because one is available (see section 80 of the 2000 Act).The use or conduct of a CHIS, however, can be a particularly intrusive and high risk covert technique, requiring dedicated and sufficient resources, oversight and management. This will include ensuring that all use or conduct is:

- necessary and proportionate to the intelligence dividend that it seeks to achieve;
- in compliance with relevant Articles of the European Convention on Human Rights, particularly Articles 6 and 8.

2.10. Unlike directed surveillance, which relates specifically to private information, authorisations for the use or conduct of a CHIS do not relate specifically to private information, but to the covert manipulation of a relationship to gain any information. ECHR case law makes it clear that Article 8 includes the right to establish and develop relationships. Accordingly, any manipulation of a relationship by a public authority (e.g. one party having a covert purpose on behalf of a public authority) is likely to engage Article 8, regardless of whether or not the public authority intends to acquire private information.

2.11. It is therefore strongly recommended that a public authority consider an authorisation whenever the use or conduct of a CHIS is likely to engage an individual's rights under Article 8, whether this is through obtaining information, particularly private information, or simply through the covert manipulation of a relationship.

Establishing, maintaining and using a relationship

2.12. The word "establishes" when applied to a relationship means "set up". It does not require, as "maintains" does, endurance over any particular period. Consequently, a relationship of seller and buyer may be deemed to exist between a shopkeeper and a customer even if only a single transaction takes place. Repetition is not always necessary to give rise to a relationship, but whether or not a relationship exists depends on all the circumstances including the length of time of the contact between seller and buyer and the nature of any covert activity.

Example 1: Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A juvenile is engaged and trained by a public authority and then deployed in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the 2000 Act that a public authority may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should be given to granting a directed surveillance authorisation.

Example 2: In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to juveniles from a room at the back of the shop, providing he has first got to know and trust them. As a consequence the public authority decides to deploy its operative on a number of occasions, to befriend the shopkeeper and gain his trust, in order to purchase

alcohol. In these circumstances a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained.

Human source activity falling outside CHIS definition

2.13. Not all human source activity will meet the definition of a CHIS. For example, a source may be a public volunteer who discloses information out of professional or statutory duty, or has been tasked to obtain information other than by way of a relationship.

Public volunteers

2.14. In many cases involving human sources, a relationship will not have been established or maintained for a covert purpose. Many sources merely volunteer or provide information that is within their personal knowledge, without being induced, asked, or tasked by a public authority. This means that the source is not a CHIS for the purposes of the 2000 Act and no authorisation under the 2000 Act is required.[7]

Example 1: A member of the public volunteers a piece of information to a member of a public authority regarding something he has witnessed in his neighbourhood. The member of the public would not be regarded as a CHIS. He is not passing information as a result of a relationship which has been established or maintained for a covert purpose.

Example 2: A caller to a confidential hotline (such as Crimestoppers, the Customs Hotline, the Anti-Terrorist Hotline, or the Security Service Public Telephone Number) reveals that he knows of criminal or terrorist activity. Even if the caller is involved in the activities on which he is reporting, the caller would not be considered a CHIS as the information is not being disclosed on the basis of a relationship which was established or maintained for that covert purpose. However, should the caller be asked to maintain his relationship with those involved and to continue to supply information, an authorisation for the use or conduct of a CHIS may be appropriate.

Professional or statutory duty

2.15. Certain individuals will be required to provide information to public authorities or designated bodies out of professional or statutory duty. For example, employees within organisations regulated by the money laundering provisions of the Proceeds of Crime Act 2002 will be required to comply with the Money Laundering Regulations 2003 and report suspicious transactions. Similarly, financial officials, accountants or company administrators may have a duty to provide information that they have obtained by virtue of their position to the Serious Fraud Office.

2.16. Any such regulatory or professional disclosures should not result in these individuals meeting the definition of a CHIS, as the business or professional relationships from which the information derives will not have been established or maintained for the covert purpose of disclosing such information.

2.17. Furthermore, this reporting is undertaken 'in accordance with the law' and any action likely to interfere with an individual's privacy, will not engage a persons human rights by virtue of Article 8(2) ECHR.

[7] See Chapter 2 of this code for further guidance on types of source activity to which authorisations under Part II of the 2000 Act may or may not apply.

2.18. This statutory or professional duty, however, would not extend to the situation where a person is asked to provide information which they acquire as a result of an existing professional or business relationship with the subject but that person is under no obligation to pass it on. For example, a travel agent who is asked by the police to find out when a regular client next intends to fly to a particular destination is not under an obligation to pass this information on. In these circumstances a CHIS authorisation may be appropriate.

Tasking not involving relationships

2.19. Tasking a person to obtain information covertly may result in authorisation under Part II of the 2000 Act being appropriate. However, this will not be true in all circumstances. For example, where the tasking given to a person does not require that person to establish or maintain a relationship for the purpose of obtaining, providing access to or disclosing the information sought or where the information is already within the personal knowledge of the individual, that person will not be a CHIS.

Example: A member of the public is asked by a member of a public authority to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, directed surveillance may need to be considered where there is an interference with the Art 8 rights of an individual

Identifying when a human source becomes a CHIS

2.20. Individuals or members of organisations (e.g. travel agents, housing associations and taxi companies) who, because of their work or role have access to personal information, may voluntarily provide information to the police on a repeated basis and need to be managed appropriately. Public authorities must keep such human sources under constant review to ensure that they are managed with an appropriate level of sensitivity and confidentiality, and to establish whether, at any given stage, they should be authorised as a CHIS.

2.21. Determining the status of an individual or organisation is a matter of judgement by the public authority. Public authorities should avoid inducing individuals to engage in the conduct of a CHIS either expressly or implicitly without obtaining a CHIS authorisation.

Example: Mr Y volunteers information to a member of a public authority about a work colleague out of civic duty. Mr Y is not a CHIS at this stage as he has not established or maintained (or been asked to establish or maintain) a relationship with his colleague for the covert purpose of obtaining and disclosing information. However, Mr Y is subsequently contacted by the public authority and is asked if he would ascertain certain specific information about his colleague. At this point, it is likely that Mr Y's relationship with colleague is being maintained and used for the covert purpose of providing that information. A CHIS authorisation would therefore be appropriate to authorise interference with the Article 8 right to respect for private and family life of Mr Y's work colleague.

2.22. However, the tasking of a person should not be used as the sole benchmark in seeking a CHIS authorisation. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised by the 2000 Act, whether or not that CHIS is asked to do so by a public authority. It is possible therefore that a person will become engaged in the conduct of a

CHIS without a public authority inducing, asking or assisting the person to engage in that conduct.

3. General rules on authorisations

Authorising Officer

3.1. Responsibility for giving the authorisation will depend on which public authority is responsible for the CHIS. For the purposes of this and future chapters, the person in a public authority responsible for granting an authorisation will be referred to as the "authorising officer". The relevant public authorities and authorising officers are listed in the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010.

Necessity and Proportionality

3.2. The 2000 Act stipulates that the authorising officer must believe that an authorisation for the use or conduct of a CHIS is necessary in the circumstances of the particular case for one or more of the statutory grounds listed in section 29(3) of the 2000 Act.

3.3. If the use or conduct of the CHIS is deemed necessary, on one of more of the statutory grounds, the person granting the authorisation must also believe that it is proportionate to what is sought to be achieved by carrying it out. This involves balancing the seriousness of the intrusion into the private or family life of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

3.4. The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render the use or conduct of a CHIS proportionate. Similarly, an offence may be so minor that any deployment of a CHIS would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

3.5. The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

Extent of authorisations

3.6. An authorisation under Part II of the 2000 Act for the use or conduct of a CHIS will provide lawful authority for any such activity that:

- involves the use or conduct of a CHIS as is specified or described in the authorisation;
- is carried out by or in relation to the person to whose actions as a CHIS the authorisation relates; and

- is carried out for the purposes of, or in connection with, the investigation or operation so described.[8]

3.7. In the above context, it is important that the CHIS is fully aware of the extent and limits of any conduct authorised and that those involved in the use of a CHIS are fully aware of the extent and limits of the authorisation in question.

Collateral Intrusion

3.8. Before authorising the use or conduct of a source, the authorising officer should take into account the risk of interference with the private and family life of persons who are not the intended subjects of the CHIS activity (collateral intrusion).

3.9. Measures should be taken, wherever practicable, to avoid or minimize interference with the private and family life of those who are not the intended subjects of the CHIS activity. Where such collateral intrusion is unavoidable, the activities may still be authorised providing this collateral intrusion is considered proportionate to the aims of the intended intrusion. Any collateral intrusion should be kept to the minimum necessary to achieve the objective of the operation.

3.10. All applications should therefore include an assessment of the risk of any collateral intrusion, and details of any measures taken to limit this, to enable the authorising officer fully to consider the proportionality of the proposed use or conduct of a CHIS.

3.11. Where CHIS activity is deliberately proposed against individuals who are not suspected of direct or culpable involvement in the matter being investigated, interference with the private and family life of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such interference should be carefully considered against the necessity and proportionality criteria as described above.

Example 1: An undercover operative is deployed to obtain information about the activities of a suspected criminal gang under CHIS authorisation. It is assessed that the operative will in the course of this deployment obtain private information about some individuals who are not involved in criminal activities and are of no interest to the investigation. The authorising officer should consider the proportionality of this collateral intrusion, and whether sufficient measures are to be taken to limit it, when granting the authorisation.

Example 2: The police seek to establish the whereabouts of Mr W in the interests of national security. In order to do so, an undercover operative is deployed to seek to obtain this information from Mr P, an associate of Mr W who is not of direct security interest. An application for a CHIS authorisation is made to authorise the deployment. The authorising officer will need to consider the necessity and proportionality of the operation against Mr P and Mr W, who will be the direct subjects of the intrusion. The authorising officer will also need to consider the proportionality of any collateral intrusion that will arise if there is any additional interference with the private and family life of other individuals of no interest to the investigation.

Reviewing and renewing authorisations

[8] See section 29(4) of the 2000 Act.

3.12. Where possible, the authorising officer who grants an authorisation should be responsible for considering subsequent renewals of that authorisation and any related security and welfare issues.

3.13. The authorising officer will stipulate the frequency of formal reviews and the controller (see paragraph 6.9 below) should maintain an audit of case work sufficient to ensure that the use or conduct of the CHIS remains within the parameters of the extant authorisation. This will not prevent additional reviews being conducted by the authorising officer in response to changing circumstances such as described below.

3.14. Where the nature or extent of intrusion into the private or family life of any person becomes greater than that anticipated in the original authorisation, the authorising officer should immediately review the authorisation and reconsider the proportionality of the operation. This should be highlighted at the next renewal.

3.15. Where a CHIS authorisation provides for interference with the private and family life of initially unidentified individuals whose identity is later established, a new authorisation is not required provided the scope of the original authorisation envisaged interference with the private and family life of such individuals.

Example: An authorisation is obtained by the police to authorise a CHIS to use her relationship with "Mr X and his close associates" for the covert purpose of providing information relating to their suspected involvement in a crime. Mr X introduces the CHIS to Mr A, a close associate of Mr X. It is assessed that obtaining more information on Mr A will assist the investigation. The CHIS may use her relationship with Mr A to obtain such information but the review of the authorisation should specify any interference with the private and family life of "Mr X and his associates, including Mr A" and that such an interference is in accordance with the original authorisation.

3.16. Any proposed changes to the *nature* of the CHIS operation (i.e. the activities involved) should immediately be brought to the attention of the authorising officer. The authorising officer should consider whether the proposed changes are within the scope of the existing authorisation and whether they are proportionate (bearing in mind any extra interference with private or family life or collateral intrusion), before approving or rejecting them. Any such changes should be highlighted at the next renewal.

Local considerations and community impact assessments

3.17. Any person granting or applying for an authorisation will also need to be aware of any particular sensitivities in the local community where the CHIS is being used and of similar activities being undertaken by other public authorities which could have an impact on the deployment of the CHIS. Consideration should also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a CHIS or use of information obtained from that CHIS.

3.18. It is therefore recommended that where an authorising officer from a public authority considers that conflicts might arise they should, where possible, consult a senior officer within the police force area in which the CHIS is deployed. All public authorities, where possible, should consider consulting with other relevant public authorities to gauge community impact.

Combined authorisations

3.19. A single authorisation may combine two or more different authorisations under Part II of the 2000 Act[9]. For example, a single authorisation may combine authorisations for intrusive surveillance and the conduct of a CHIS. In such cases the provisions applicable to each of the authorisations must be considered separately by the appropriate authorising officer. Thus, a police superintendent, or above, can authorise the conduct of a CHIS but an authorisation for intrusive surveillance by the police needs the separate authorisation of a chief constable (and the prior approval of a Surveillance Commissioner, except in cases of urgency).

3.20. Where an authorisation for the use or conduct of a CHIS is combined with a Secretary of State authorisation for intrusive surveillance, the combined authorisation must be issued by the Secretary of State.

3.21. The above considerations do not preclude public authorities from obtaining separate authorisations.

Operations involving multiple CHIS

3.22. A single authorisation under Part II of the 2000 Act may be used to authorise more than one CHIS. However, this is only likely to be appropriate for operations involving the conduct of several undercover operatives acting as CHISs in situations where the activities to be authorised, the subjects of the operation, the interference with private and family life, the likely collateral intrusion and the environmental or operational risk assessments are the same for each officer.

Covert surveillance of a potential CHIS

3.23. It may be necessary to deploy covert surveillance against a potential CHIS, other than those acting in the capacity of an undercover operative, as part of the process of assessing their suitability for recruitment, or in planning how best to make the approach to them. Covert surveillance in such circumstances may or may not be necessary on one of the statutory grounds on which directed surveillance authorisations can be granted, depending on the facts of the case. Whether or not a directed surveillance authorisation is available, any such surveillance must be justifiable under Article 8(2) of the ECHR.

Use of covert human intelligence source with technical equipment

3.24. A CHIS wearing or carrying a surveillance device does not need a separate intrusive or directed surveillance authorisation, provided the device will only be used in the presence of the CHIS. However, if a surveillance device is to be used other than in the presence of the CHIS, an intrusive or directed surveillance authorisation should be obtained where appropriate, together with an authorisation for interference with property, if applicable. See the Covert Surveillance and Property Interference Code of Practice.

3.25. A CHIS, whether or not wearing or carrying a surveillance device, in residential premises or a private vehicle, does not require additional authorisation to record any activity taking place inside those premises or that vehicle which takes place in his presence. This also applies to the recording of telephone conversations or other forms of communication, other than by interception, which takes place in the source's presence. Authorisation for the use or conduct of that source may be obtained in the usual way.

[9] See section 43(2) of the 2000 Act.

Oversight of use of covert human intelligence sources by local authorities

3.26. Elected members of a local authority should review the authority's use of the 2000 Act and set the policy at least once a year. They should also consider internal reports on use of the 2000 Act on at least a quarterly basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose. They should not, however, be involved in making decisions on specific authorisations.

4. Special considerations for authorisations

Legally privileged material and other confidential information

4.1. The 2000 Act does not provide any special protection for 'confidential information'. Nevertheless, particular care should be taken in cases where the subject of the intrusion might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information, confidential constituent information or confidential journalistic material. So, for example, extra care should be taken where, through the use or conduct of a CHIS, it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or between a Member of Parliament and a constituent relating to private constituency matters, or wherever matters of medical or journalistic confidentiality or legal privilege may be involved. References to a Member of Parliament include references to Members of both Houses of the UK Parliament, the European Parliament, the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly.

4.2. In cases where through the use or conduct of a CHIS it is likely that knowledge of legally privileged material or other confidential information will be acquired, the deployment of the CHIS is subject to a higher level of authorisation. The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 lists the authorising officer for each public authority permitted to authorise such use or conduct of a CHIS.

Matters subject to Legal Privilege - Introduction

4.3. Section 98 of the 1997 Act defines those matters that are subject to legal privilege. Under this definition, legal privilege does not apply to communications or items held, or oral communications made, with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if the professional legal adviser is intending to hold or use them for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence.

4.4. Public authorities may obtain knowledge of matters subject to legal privilege via CHIS in three scenarios: first, where the public authority responsible for the CHIS deliberately authorised the use or conduct of the CHIS in order to obtain knowledge of matters subject to legal privilege; second, where the CHIS obtains knowledge of matters subject to legal privilege through conduct incidental (within the meaning of section 26(7)(a)) to his conduct as a CHIS; and, third, where a CHIS obtains knowledge of matters subject to legal privilege where his conduct cannot properly be regarded as incidental to his conduct as a CHIS. Separate guidance is relevant to each scenario.

Authorisations for the use or conduct of a CHIS to obtain, provide access to or disclose knowledge of matters subject to legal privilege

4.5. If a public authority seeks to grant or renew an authorisation for the use or conduct of a CHIS in order to obtain, provide access to or disclose knowledge of matters subject to legal privilege, the 2009 Order will apply. The 2009 Order creates an enhanced regime of prior approval for such authorisations. The 2009 Order provides that before an authorising officer grants or renews an authorisation to which the Order applies, he must give notice to the relevant approving officer. The relevant approving officer will be the Secretary of State in the case of a member of the intelligence services, an official of the Ministry of Defence, an individual holding an office, rank or position in Her Majesty's Prison Service or the Northern Ireland Prison Service. In all other cases, the relevant approving officer will be an ordinary Surveillance Commissioner. The authorising

officer is prohibited from granting or renewing an authorisation to which the 2009 Order applies until he has received confirmation in writing that the approving officer has approved the application. If the approving officer does not approve the application, the authorising officer may still grant an authorisation in respect of the use or conduct of the CHIS in question, but may not authorise the use or conduct of the CHIS to obtain, provide access to or disclose knowledge of matters subject to legal privilege.

4.6. Approving officers may only approve, and authorising officers may only authorise, the use or conduct of CHIS to acquire knowledge of matters subject to legal privilege if they are satisfied that there are exceptional and compelling circumstances that make the authorisation necessary. Such circumstances will arise only in a very restricted range of cases, such as where there is a threat to life or limb, or to national security, and the use or conduct of a CHIS to acquire knowledge of matters subject to legal privilege is reasonably regarded as likely to yield intelligence necessary to counter the threat.

Circumstances in which the obtaining of knowledge of matters subject to legal privilege by a CHIS or public authority is incidental to the conduct authorised in the authorisation

4.7. The reactive nature of the work of a CHIS, and the need for a CHIS to maintain cover, may make it necessary for a CHIS to engage in conduct which was not envisaged at the time the authorisation was granted, but which is incidental to that conduct. Such incidental conduct is regarded as properly authorised by virtue of sections 26(7)(a), 27 and 29(4) of the 2000 Act, even though it was not specified in the initial authorisation.

4.8. This is likely to occur only in exceptional circumstances, such as where the obtaining of such knowledge is necessary to protect life and limb, including in relation to the CHIS, or national security, in circumstances that were not envisaged at the time the authorisation was granted.

4.9. If any of these situations arise, the public authority should draw it to the attention of the relevant Commissioner or Inspector during his next inspection (at which the material should be made available if requested). In addition, the public authority in question should ensure that any knowledge of matters subject to legal privilege obtained through conduct incidental to the use or conduct of a CHIS specified in the authorisation is not used in law enforcement investigations or criminal prosecutions.

4.10. If it becomes apparent that it will be necessary for the CHIS to continue to obtain, provide access to or disclose knowledge of matters subject to legal privilege, the initial authorisation should be replaced by an authorisation that has been subject to the prior approval procedure set out in the 2009 Order at the earliest reasonable opportunity.

Unintentional obtaining of knowledge of matters subject to legal privilege by a CHIS

4.11. Public authorities should make every effort to avoid their CHIS unintentionally obtaining, providing access to or disclosing knowledge of matters subject to legal privilege. If a public authority assesses that a CHIS may be exposed to such knowledge unintentionally, the public authority should task the CHIS in such a way that this possibility is reduced as far as possible. When debriefing the CHIS, the public authority should make every effort to ensure that any knowledge of matters subject to legal privilege which the CHIS may have obtained is not disclosed to the public authority, unless there are exceptional and compelling circumstances that make such disclosure necessary. If, despite these steps, knowledge of matters subject to legal privilege is unintentionally disclosed to the public authority, the public authority in question should ensure that it is not used in law enforcement investigations or criminal prosecutions. Any unintentional obtaining of knowledge of matters subject to legal privilege by a public authority, together with a

description of all steps taken in relation to that material, should be drawn to the attention of the relevant Commissioner or Inspector during his next inspection (at which the material should be made available if requested).

The use and handling of material subject to legal privilege

4.12. Legally privileged information is particularly sensitive and any use or conduct of CHIS which obtains, provides access to or discloses such material may give rise to issues under Article 6 of the ECHR (right to a fair trial) as well as engaging Article 8.

4.13. Where public authorities deliberately obtain knowledge of matters subject to legal privilege via the conduct of a CHIS, they may use it to counter the threat which led them to obtain it; but not for other purposes. In particular, public authorities should ensure that knowledge of matters subject to legal privilege is kept separate from law enforcement investigations or criminal prosecutions.

4.14. In cases likely to result in the obtaining by a public authority of knowledge of matters subject to legal privilege, the authorising officer or Surveillance Commissioner may require regular reporting so as to be able to decide whether the authorisation should continue. In those cases where knowledge of matters subject to legal privilege has been obtained and retained, the matter should be reported to the authorising officer by means of a review and to the relevant Commissioner or Inspector during his next inspection (at which the material should be made available if requested).

4.15. A substantial proportion of the communications between a lawyer and his client(s) may be subject to legal privilege. Therefore, in any case where a lawyer is the subject of an investigation or operation, authorising officers should consider whether the special safeguards outlined in this chapter apply. Any material which has been retained from any such investigation or operation should be notified to the relevant Commissioner or Inspector during his next inspection and made available on request.

4.16. Where there is any doubt as to the handling and dissemination of information which may be subject to legal privilege, advice should be sought from a legal adviser within the relevant public authority before any further dissemination of the material takes place. Similar advice should also be sought where there is doubt over whether information is not subject to legal privilege due to the "in furtherance of a criminal purpose" exception. The retention of legally privileged information, or its dissemination to an outside body, should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to ensure there is no possibility of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates. Any dissemination of legally privileged material to an outside body should be notified to the relevant Commissioner or Inspector during his next inspection.

Confidential Information

4.17. Similar consideration must also be given to authorisations for use or conduct that are likely to result in the obtaining of confidential personal information, confidential constituent information and confidential journalistic material. Where such material has been acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during his next inspection and the material be made available to him if requested.

4.18. Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified

from it.[10] Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records.

4.19. Confidential constituent information is information held in confidence in relation to communications between a Member of Parliament and a constituent in respect of constituency matters. Again, such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

4.20. Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

4.21. Where there is any doubt as to the handling and dissemination of confidential information, advice should be sought from a legal adviser, who is independent from the investigation, within the relevant public authority before any further dissemination of the material takes place. Any dissemination of confidential material to an outside body should be notified to the relevant Commissioner or Inspector during his next inspection.

Vulnerable individuals

4.22. A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description should only be authorised to act as a CHIS in the most exceptional circumstances. In these cases, Annex A lists the authorising officer for each public authority permitted to authorise the use of a vulnerable individual as a CHIS.

Juvenile sources

4.23. Special safeguards also apply to the use or conduct of juveniles, that is, those under 18 years old, as sources. On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him. In other cases, authorisations should not be granted unless the special provisions contained within The Regulation of Investigatory Powers (Juveniles) Order 2000; SI No. 2793 are satisfied. Authorisations for juvenile sources should be granted by those listed in the attached table at Annex A. The duration of such an authorisation is one month from the time of grant or renewal (instead of twelve months). For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

Scotland

4.24. Where all the conduct authorised is likely to take place in Scotland, authorisations should be granted under RIP(S)A, unless:

[10] **Spiritual counselling** means conversations between a person and a religious authority acting in an official capacity, where the individual being counselled is seeking or the religious authority is imparting forgiveness, absolution or the resolution of conscience in accordance with their faith.

- the authorisation is being obtained by those public authorities listed in section 46(3) of the 2000 Act and the Regulation of Investigatory Powers (Authorisations Extending to Scotland) Order 2000; SI No. 2418;

- the authorisation is to be granted or renewed (by any relevant public authority) for the purposes of national security or the economic well-being of the UK; or

- the authorisation authorises conduct that is surveillance by virtue of section 48(4) of the 2000 Act.

4.25. This code of practice is extended to Scotland in relation to authorisations granted under Part II of the 2000 Act which apply to Scotland. A separate code of practice applies in relation to authorisations granted under RIP(S)A.

International

4.26. Authorisations under the 2000 Act can be given for the use or conduct of CHIS both inside and outside the UK. However, authorisations for actions outside the UK can usually only validate them for the purposes of UK law.

4.27. Public authorities are therefore advised to seek authorisations where available under the 2000 Act for any overseas operations where the subject of investigation is a UK national or is likely to become the subject of criminal or civil proceedings in the UK, or if the operation is likely to affect a UK national or give rise to material likely to be used in evidence before a UK court.

4.28. Public authorities must have in place internal systems to manage any overseas CHIS deployments and it is recognised practice for UK law enforcement agencies to follow the authorisation and management regime under the 2000 Act, even where such deployments are only intended to impact locally and are therefore authorised under domestic law. However, public authorities should take care to monitor such deployments to identify where civil or criminal proceedings may become a prospect in the UK and ensure that, where appropriate, an authorisation under Part II of the 2000 Act is sought if this becomes the case.

4.29. The Human Rights Act 1998 applies to all activity taking place within the UK. This should be taken to include overseas territories and facilities which are within the jurisdiction of the UK. Authorisations under the 2000 Act may therefore be appropriate for overseas covert operations occurring in UK Embassies, military bases, detention facilities, etc., in order to comply with rights to privacy under Article 8 of the ECHR.[11]

4.30. Members of foreign law enforcement or other agencies or CHIS of those agencies may be authorised under the 2000 Act in the UK in support of domestic and international investigations.

[11] See R v Al Skeini June 2007. If conduct is to take place overseas the ACPO Covert Investigation (Legislation and Guidance) Steering Group may be able to offer additional advice.

5. Authorisation procedures for covert human intelligence sources

Authorisation criteria

5.1. Under section 29(3) of the 2000 Act an authorisation for the use or conduct of a CHIS may be granted by the authorising officer where he believes that the authorisation is necessary:

- in the interests of national security[12];
- for the purpose of preventing or detecting[13] crime or of preventing disorder;
- in the interests of the economic well-being of the UK;
- in the interests of public safety;
- for the purpose of protecting public health[14];
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or for any other purpose prescribed in an order made by the Secretary of State[15].

5.2. The authorising officer must also believe that the authorised use or conduct of CHIS is proportionate to what is sought to be achieved by that use or conduct.

Relevant public authorities

5.3. The public authorities entitled to authorise the use or conduct of a CHIS, together with the specific purposes for which each public authority may authorise the use or conduct of a CHIS, are laid out in Schedule 1 of the 2000 Act and the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010.

Authorisation procedures

5.4. Responsibility for authorising the use or conduct of a CHIS rests with the authorising officer and all authorisations require the personal authority of the authorising officer. The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 designates the authorising officer for each different public authority and the officers entitled to act only in urgent cases. In certain circumstances the Secretary of State will be the authorising officer (see section 30(2) of the 2000 Act).

5.5. The authorising officer must give authorisations in writing, except in urgent cases, where they may be given orally. In such cases, a statement that the authorising officer has expressly authorised the action should be recorded in writing by the applicant (or the person with whom the authorising officer spoke) as a priority. This statement need not contain the full detail of the

---

[12] One of the functions of the Security Service is the protection of national security and in particular the protection against threats from terrorism. These functions extend throughout the UK. An authorising officer in another public authority should not issue an authorisation under Part II of the 2000 Act where the operation or investigation falls within the responsibilities of the Security Service, as set out above, except where it is to be carried out by a Special Branch, Counter Terrorist Unit or where the Security Service has agreed that another public authority can authorise the use or conduct of a CHIS which would normally fall within the responsibilities of the Security Service. HM Forces may also undertake operations in connection with national security in support of the Security Service or other Civil Powers.

[13] Detecting crime is defined in section 81(5) of the 2000 Act. Preventing and detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences.

[14] This could include investigations into infectious diseases, contaminated products or the illicit sale of pharmaceuticals.

[15] This could only be for a purpose which satisfies the criteria set out in Article 8(2) of the ECHR.

application, which should however subsequently be recorded in writing when reasonably practicable (generally the next working day).

5.6. Other officers entitled to act in urgent cases may only give authorisation in writing e.g. written authorisation for directed surveillance given by an Inspector.

5.7. A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the operation or investigation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the applicant's or authorising officer's own making.

5.8. Authorising officers should not be responsible for authorising their own activities, e.g. those in which they, themselves, are to act as the CHIS or as the handler of the CHIS. Furthermore, authorising officers should, where possible, be independent of the investigation. However, it is recognised that this is not always possible, especially in the cases of small organisations, or where it is necessary to act urgently or for security reasons. Where an authorising officer authorises his own activity the central record of authorisations should highlight this and the attention of a Commissioner or Inspector should be invited to it during his next inspection.

5.9. Authorising officers within the SCDEA and SOCA may only grant authorisations on application by a member of (including those formally seconded to) their own force or agency. The same rules applies to authorising officers within police forces, unless relevant Chief Officers have made collaboration agreements under section 23 of the Police Act 1996 or section 12 of the Police (Scotland) Act 1967 which permit authorising officers to grant authorisations on application from members of other forces. Authorising officers within HMRC may only grant authorisations on application by an officer of Revenues and Customs.

Information to be provided in applications for authorisation

5.10. An application for authorisation for the use or conduct of a CHIS should be in writing and record:

- the reasons why the authorisation is necessary in the particular case and on the grounds listed in section 29(3) of the 2000 Act (e.g. for the purpose of preventing or detecting crime);
- the purpose for which the CHIS will be tasked or deployed (e.g. in relation to drug supply, stolen property, a series of racially motivated crimes etc);
- where a specific investigation or operation is involved, the nature of that investigation or operation;
- the nature of what the CHIS conduct will be;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the authorisation;
- the reasons why the authorisation is considered proportionate to what it seeks to achieve;
- the level of authorisation required (or recommended, where that is different); and

- a subsequent record of whether authorisation was given or refused, by whom and the time and date.

5.11. Additionally, in urgent cases, the authorisation should record (as the case may be):

- the reasons why the authorising officer considered the case so urgent that an oral instead of a written authorisation was given ; or
- the reasons why the officer entitled to act in urgent cases considered the case so urgent and why it was not reasonably practicable for the application to be considered by the authorising officer.

5.12. Where the authorisation is oral, the detail referred to above should be recorded in writing by the applicant when reasonably practicable (generally the next working day).

Duration of authorisations

5.13. A written authorisation will, unless renewed, cease to have effect at the end of a period of twelve months beginning with the day on which it took effect, except in the case of juvenile CHIS.

5.14. Urgent oral authorisations or authorisations granted or renewed by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after seventy-two hours, beginning with the time when the authorisation was granted.

Reviews

5.15. Regular reviews of authorisations should be undertaken by the authorising officer to assess whether it remains necessary and proportionate to use a CHIS and whether the authorisation remains justified. The review should include the use made of the CHIS during the period authorised, the tasks given to the CHIS and the information obtained from the CHIS. The results of a review should be retained for at least three years (see chapter 7). Particular attention is drawn to the need to review authorisations frequently where the use of a CHIS provides access to confidential information or involves significant collateral intrusion.

5.16. In each case the authorising officer within each public authority should determine how often a review should take place. This should be as frequently as is considered necessary and practicable, but should not prevent reviews being conducted in response to changing circumstances.

Renewals

5.17. Before an authorising officer renews an authorisation, he must be satisfied that a review has been carried out of the use of a CHIS, as outlined above, and that the results of the review have been considered.

5.18. If, before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for a further period of twelve months. Renewals may also be granted orally in urgent cases and last for a period of seventy-two hours.

5.19. A renewal takes effect at the time at which the authorisation would have ceased to have effect but for the renewal. An application for renewal should therefore not be made until shortly before the authorisation period is drawing to an end.

5.20. Any person who would be entitled to grant a new authorisation can renew an authorisation. However, where possible the authorising officer who granted the original authorisation should consider the renewal.

5.21. Authorisations may be renewed more than once, if necessary, provided they continue to meet the criteria for authorisation. Documentation of the renewal should be retained for at least three years (see Chapter 7).

5.22. All applications for the renewal of an authorisation should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information in the initial application;
- the reasons why it is necessary for the authorisation to continue;
- the use made of the CHIS in the period since the grant or, as the case may be, latest renewal of the authorisation;
- the tasks given to the CHIS during that period and the information obtained from the use or conduct of the CHIS; and
- the results of regular reviews of the use of the CHIS.

Cancellations

5.23. The authorising officer who granted or renewed the authorisation must cancel it if he is satisfied that the use or conduct of the CHIS no longer satisfies the criteria for authorisation or that arrangements for the CHIS's case no longer satisfy the requirements described in section 29 of the 2000 Act. Where the authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer or the person who is acting as authorising officer.

5.24. Where necessary, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled.

6. Management of covert human intelligence sources

Tasking

6.1. Tasking is the assignment given to the CHIS by the persons defined at sections 29(5)(a) and (b) of the 2000 Act, asking him to obtain, provide access to or disclose information. Authorisation for the use or conduct of a CHIS will be appropriate prior to any tasking where such tasking involves the CHIS establishing or maintaining a personal or other relationship for a covert purpose.

6.2. Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If the nature of the task changes significantly, then a new authorisation may need to be sought.

6.3. It is difficult to predict exactly what might occur each time a meeting with a CHIS takes place, or the CHIS meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, the occurrence must be recorded as soon as practicable after the event and if the existing authorisation is insufficient it should either be updated at a review (for minor amendments only) or it should be cancelled and a new authorisation should be obtained before any further such action is carried out.

6.4. Similarly, where it is intended to task a CHIS in a significantly greater or different way than previously identified, the persons defined at section 29(5)(a) or (b) of the 2000 Act must refer the proposed tasking to the authorising officer, who should consider whether the existing authorisation is sufficient or needs to be replaced. This should be done in advance of any tasking and the details of such referrals must be recorded. Efforts should be made to minimise the number of authorisations per CHIS to the minimum necessary in order to avoid generating excessive paperwork.

Handlers and controllers

6.5. Public authorities should ensure that arrangements are in place for the proper oversight and management of CHIS, including appointing individual officers as defined in section 29(5)(a) and (b) of the 2000 Act for each CHIS.

6.6. Oversight and management arrangements for undercover operatives, while following the principles of the Act, will differ, in order to reflect the specific role of such individuals as members of public authorities.

6.7. The person referred to in section 29(5)(a) of the 2000 Act (the "handler") will have day to day responsibility for:

- dealing with the CHIS on behalf of the authority concerned;
- directing the day to day activities of the CHIS;
- recording the information supplied by the CHIS; and
- monitoring the CHIS's security and welfare.

6.8. The handler of a CHIS will usually be of a rank or position below that of the authorising officer.

6.9. The person referred to in section 29(5)(b) of the 2000 Act (the "controller") will normally be responsible for the management and supervision of the "handler" and general oversight of the use of the CHIS.

Joint working

6.10. In cases where the authorisation is for the use or conduct of a CHIS whose activities benefit more than a single public authority, responsibilities for the management and oversight of that CHIS may be taken up by one authority or can be split between the authorities. The controller and handler of a CHIS need not be from the same public authority.

6.11. There are many cases where the activities of a CHIS may provide benefit to more than a single public authority. Such cases may include:

- The prevention or detection of criminal matters affecting a national or regional area, for example where the CHIS provides information relating to cross boundary or international drug trafficking;

- The prevention or detection of criminal matters affecting crime and disorder, requiring joint agency operational activity, for example where a CHIS provides information relating to environmental health issues and offences of criminal damage, in a joint police/ local authority anti-social behaviour operation on a housing estate;

- Matters of national security, for example where the CHIS provides information relating to terrorist activity and associated criminal offences for the benefit of the police and the Security Service.

6.12. In such situations, however, the public authorities involved must lay out in writing their agreed oversight arrangements.

6.13. Management responsibility for CHIS, and relevant roles, may also be divided between different police forces where the Chief Officers of the forces concerned have made a collaboration agreement under section 23 of the Police Act 1996 or section 12 of the Police (Scotland) Act 1967, and the collaboration agreement provides for this to happen.

Security and welfare

6.14. Any public authority deploying a CHIS should take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking. Before authorising the use or conduct of a CHIS, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset. Also, consideration should be given to the management of any requirement to disclose information tending to reveal the existence or identity of a CHIS to, or in, Court.

6.15. The CHIS handler is responsible for bringing to the attention of the CHIS controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

- the validity of the risk assessment;
- the conduct of the CHIS; and
- the safety and welfare of the CHIS.

6.16. Where appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue.

7. Keeping of records

Centrally retrievable record of authorisations

7.1. A centrally retrievable record of all authorisations should be held by each public authority. These records need only contain the name, code name, or unique identifying reference of the CHIS, the date the authorisation was granted, renewed or cancelled and an indication as to whether the activities were self-authorised. These records should be updated whenever an authorisation is granted, renewed or cancelled and should be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners upon request. These records should be retained for a period of at least three years from the ending of the authorisations to which they relate.

7.2. While retaining such records for the time stipulated, public authorities must take into consideration the duty of care to the CHIS, the likelihood of future criminal or civil proceedings relating to information supplied by the CHIS or activities undertaken, and specific rules relating to data retention, review and deletion under the Data Protection Act and, where applicable, the Code of Practice on the Management of Police Information.

Individual records of authorisation and use of CHIS

7.3. Detailed records must be kept of the authorisation and use made of a CHIS. Section 29(5) of the 2000 Act provides that an authorising officer must not grant an authorisation for the use or conduct of a CHIS unless he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS. The Regulation of Investigatory Powers (Source Records) Regulations 2000; SI No: 2725 details the particulars that must be included in these records.

7.4. Public authorities are encouraged to consider maintaining such records also for human sources who do not meet the definition of a CHIS. This may assist authorities to monitor the status of a human source and identify whether that source becomes a CHIS.

Further documentation

7.5. In addition, records or copies of the following, as appropriate, should be kept by the relevant authority for at least three years:

- a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing an authorisation considered it necessary to do so;
- any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- any risk assessment made in relation to the CHIS;
- the circumstances in which tasks were given to the CHIS;
- the value of the CHIS to the investigating authority;
- a record of the results of any reviews of the authorisation;

- the reasons, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation; and
- the date and time when any instruction was given by the authorising officer that the conduct or use of a CHIS must cease.

7.6. The records kept by public authorities should be maintained in such a way as to preserve the confidentiality, or prevent disclosure of the identity of the CHIS, and the information provided by that CHIS.

8. Handling of material

Retention and destruction of material

8.1. Each public authority must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use or conduct of a CHIS. Authorising officers must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

8.2. Where the product of the use or conduct of a CHIS could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with applicable disclosure requirements.

8.3. Subject to the provisions in Chapter 4 above, there is nothing in the 2000 Act or this Code of Practice which prevents material obtained from authorisations for the use or conduct of a CHIS for a particular purpose from being used to further other purposes.

Law enforcement agencies

8.4. In the cases of the law enforcement agencies, particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

The intelligence services, MOD and HM Forces

8.5. The heads of these agencies are responsible for ensuring that arrangements exist to make sure that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure. For the intelligence services, this is a statutory duty under the 1989 Act and the 1994 Act.

8.6. With regard to the service police forces (the Royal Navy Police, the Royal Military Police and the Royal Air Force Police), particular attention is drawn to the Criminal Procedure and Investigations Act 1996 (Code of Practice) (Armed Forces) Order 2008, which requires that the investigator retain all material obtained in a service investigation which may be relevant to the investigation.

Use of material as evidence

8.7. Subject to the provisions in Chapter 4 above, material obtained from a CHIS may be used as evidence in criminal proceedings[16]. The admissibility of evidence is governed by the common law, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984[17] and the Human Rights Act 1998. Whilst this code does not affect the application of those rules, obtaining appropriate authorisations should help ensure the admissibility of evidence derived from CHIS.

[16] whether these proceedings are brought by the public authority that obtained the authorisation or by another public authority (subject to handling arrangements agreed between the authorities)

[17] and section 76 of the Police & Criminal Evidence (Northern Ireland) Order 1989

8.8. Product obtained by a CHIS is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996, where those rules apply to the law enforcement body in question.

8.9. There are also well-established legal procedures under public interest immunity provisions that can be applied when seeking to protect the identity of a source from disclosure in such circumstances.

9. Senior responsible officers and oversight by Commissioners

The senior responsible officer

9.1. Within every relevant public authority a senior responsible officer must be responsible for:

- the integrity of the process in place within the public authority for the management of CHIS;
- compliance with Part II of the Act and with this code;
- oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the OSC inspectors when they conduct their inspections, where applicable; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

9.2. Within local authorities, the senior responsible officer should be a member of the corporate leadership team and should be responsible for ensuring that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of the Surveillance Commissioner. Where an inspection report highlights concerns about the standards of authorising officers, this individual will be responsible for ensuring the concerns are addressed.

Oversight by Commissioners

9.3. The 2000 Act requires the Chief Surveillance Commissioner to keep under review (with the assistance of the Surveillance Commissioners and Assistant Surveillance Commissioners) the performance of functions under Part III of the 1997 Act and Part II of the 2000 Act by the police (including the service police forces, the Ministry of Defence Police and the British Transport Police), SOCA, SCDEA, HMRC and the other public authorities listed in Schedule 1 of the 2000 Act and the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, and in Northern Ireland officials of the Ministry of Defence and HM Forces.

9.4. The Intelligence Services Commissioner's remit is to provide independent oversight of the use of Part II of the 2000 Act and the 1994 Act by the Security Service, Secret Intelligence Service, GCHQ and the Ministry of Defence and HM Forces (excluding the service police forces, and in Northern Ireland officials of the Ministry of Defence and HM Forces).

9.5. This code does not cover the exercise of any of the Commissioners' functions. It is the duty of any person who uses Part II of RIPA to comply with any request made by a Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions.

9.6. References in this code to the performance of review functions by the Chief Surveillance Commissioner and other Commissioners apply also to Inspectors and other members of staff to whom such functions have been delegated.

9.7. Reports made by the Commissioners concerning the inspection of public authorities and their exercise and performance of powers under Part II may be made available by the

Commissioners to the Home Office to promulgate good practice and help identify training requirements within public authorities.

9.8. Subject to the approval of the relevant Commissioner public authorities may publish their inspection reports, in full or in summary, to demonstrate both the oversight to which they are subject and their compliance with Part II of the Act and this code. Approval should be sought on a case by case basis at least 10 working days prior to intended publication, stating whether the report is to be published in full, and if not stating which parts are to be published or how it is to be summarised.

10. Complaints

10.1. The 2000 Act establishes an independent Tribunal. This Tribunal will be made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction. This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

020 7035 3711

ANNEX A

Authorisation levels when knowledge of confidential information is likely to be acquired or when a vulnerable individual or juvenile is to be used as a source.

Relevant Public Authority	Authorisation level for when knowledge of Confidential Information is likely to be acquired	Authorisation level for when a vulnerable individual or a Juvenile is to be used as a source
Police Forces:		
Any police force maintained under section 2 of the Police Act 1996 (police forces in England and Wales outside London)	Chief Constable	Assistant Chief Constable
Any police force maintained under or by virtue of section 1 of the Police (Scotland) Act 1967	Chief Constable	Assistant Chief Constable
The Metropolitan police force	Assistant Commissioner	Commander
The City of London police force	Commissioner	Commander
The Police Service of Northern Ireland	Deputy Chief Constable	Assistant Chief Constable
The Ministry of Defence Police	Chief Constable	Assistant Chief Constable
The Royal Navy Police The Royal Military Police The Royal Air Force Police	Provost Marshal Provost Marshal Provost Marshal	Provost Marshal Provost Marshal Provost Marshal
The Serious Organised Crime Agency	Deputy Director	Deputy Director
The Serious Fraud Office	A Member of the Senior Civil Service or Head of Domain	A Member of the Senior Civil Service or Head of Domain
The Intelligence Services:		
The Security Service	Deputy Director General	Deputy Director General
The Secret Intelligence Service	A Director of the Secret Intelligence Service	A member of the Secret Intelligence Service not below the equivalent rank to that of a Grade 5 in the Home Civil Service

The Government Communications Headquarters	A Director of GCHQ	A Director of GCHQ
HM Forces:		
The Royal Navy	Rear Admiral	Rear Admiral
The Army	Major General	Major General
The Royal Air Force	Air-Vice Marshal	Air-Vice Marshal
The Commissioners for HM Revenue and Customs	Director Investigation, **or** Regional Heads of Investigation	Grade 7 (Intelligence)
The Department for the Environment, Food and Rural Affairs:		
DEFRA Investigation Services	Head of DEFRA Investigation Services	Head of DEFRA Investigation Services
Marine and Fisheries Agency	Head of DEFRA Prosecution Service	----------
Centre for Environment, Fisheries & Aquaculture Science	Head of DEFRA Prosecution Service	Head of DEFRA Prosecution Service
The Department of Health:		
The Medicines & Healthcare Products Regulatory Agency	Chief Executive	Head of Division for Inspection and Enforcement
The Home Office:		
The UK Border Agency	Strategic Director of the UK Border Agency, or (in his/her absence) Director of the UK Border Agency Intelligence Directorate	Strategic Director of the UK Border Agency
The Ministry of Justice	Chief Operating Officer in the National Offender Management Service	A member of the Senior Civil Service in the National Offender Management Service not below the equivalent rank of a Grade 5 in the Home Civil Service
The Northern Ireland Office:		
The Northern Ireland Prison Service	Director or Deputy Director Operations in the Northern Ireland Prison Service	Director or Deputy Director Operations in the Northern Ireland Prison Service
The Department of Business, Innovation and Skills	The Director of Legal Services A	The Director of Legal Services A
The Welsh Assembly Government	Head of Department for	Head of Department for

	Health & Social Services, Head of Department for Health & Social Services Finance, Head of Rural Payments Division, Regional Director or equivalent grade in the Care & Social Services Inspectorate for Wales	Health & Social Services Head of Department for Health & Social Services Finance, Head of Rural Payments Division, Regional Director or equivalent grade in the Care & Social Services Inspectorate for Wales
Any county council or district Council in England, a London borough council, the Common Council of the City of London in its capacity as a local authority, the Council of the Isles of Scilly, and any county council or borough council in Wales	Head of Paid Service, or (in his absence) the person acting as the Head of Paid Service	Head of Paid Service, or (in his absence) the person acting as the Head of paid Service
The Environment Agency	Chief Executive of the Environment Agency	Executive Manager in the Environment Agency
The Financial Services Authority	Chairman of the Financial Services Authority	Chairman of the Financial Services Authority
The Food Standards Agency	Head of Group, or Deputy Chief Executive or Chief Executive of the Food Standards Agency	Head of Group, or Deputy Chief Executive or Chief Executive of the Food Standards Agency
The Gambling Commission	----------	Chief Executive
The Health and Safety Executive	Director of Field Operations, or Director of Hazardous Installations Directorate, or Her Majesty's Chief Inspector of Nuclear Installations	Director of Field Operations, or Director of Hazardous Installations Directorate, or Her Majesty's Chief Inspector of Nuclear Installations